A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH

Shailendra Singh Gaur[1], Hemanpreet Singh Kalsi[2], Shivani Gautam[3]
[123]*Bhagwan Parshuram Institute of Technology (GGSIPU)*
(shailendrasinghgaur@bpitindia.com)

Abstract—Network security through cryptographic algorithm and protocols remains the best suitable method for maintaining confidentiality such that in this paper different cryptographic algorithms are compared, analysis is performed and results are obtained for further operations on the basis of outcomes.

Keywords—*Network Security; Cryptography; RSA; DES; AES; Blowfish; 3-DES*

I. INTRODUCTION

We are surrounded by electronic devices and a link of communication is being created with other devices, there can be two or more than two devices where sharing of vital data or exchange of resources occurs between them. The linking of devices itself acts as a channel between them and this linking of multiple devices together creates a network. It can be accomplished through connecting cables, radio waves, telephone lines, satellite or infra-red light. The setting up of connection and process of transmitting information has to be secure, network may be as small as a group of two devices or a large complex network comprising 'n' number of devices. So, that no unauthorized person can access or modify the data which is being transmitted within the network. The network connection can be LAN, MAN, WAN, WLAN, WMAN, but if problems occurs, entering of bugs or mal-activities causing Denial of Service attack or active attacks (such that an intruder or eaves-dropper start the commands so that it malfunctions or disrupts the basic normal network operation so that a reconnaissance takes place) and passive attacks (such that when an intruder intercept the data that might be travelling through the network) takes place, then it becomes difficult for both the service provider and client or client-client connection to be smooth and confidential maintaining integrity. Network needs security for which some policies and rules or protocols have been defined to make the misuse and unauthorized access removed and protection of the network is maintained as in [1]. The network present either publicly or privately needs to be protected and easiest way is to assign a username and password to anything that sort of needs protection but securing a transaction, or a network line that have already been provided with access through entering of these credentials might then too, be vulnerable as eaves-dropper can attack passively into the network. The data maybe passed through a station called node which are connected in different ways to each other to form a best connection making communication systems more accurate and real time transmission should be present with the precise delivery destination to which the user was intended to pass. The process of flow control manages the transmission of data between two nodes, preventing fast sender from out-passing the slow receiver, controlling the mechanism of speed transmission, making it important for sending at faster rate by the sender such that it could be processed. This flow of data could be secured using network security protocols and policies out of which the mostly used model is OSI (Open System Interconnection) model such that there are present many standards or common set of rules like IEEE (Institute of Electrical And Electronics Engineer), ANSI (American national Standard Institute), ISO (International Standard of Organization), ETSI (European Tele-communication Standard Institute), W3C (World Wide Web Consortium). Hackers or eaves-droppers maybe present who will hack the network and may breach the network or there might be possibility of bifurcation. Similarly, hiding the same can help, letting the eavesdropper difficult to interpret or get into observation. This process is called cryptography where the process is implemented through either using codes or rules of steps called algorithms.as in [1][3] These algorithms had their presence from 100BC, Julius Caesar using his logical way of arranging the letters in additive manner that may perfectly hide the real message required to be kept confidential. This same method has evolved into two methods Substitution and traditional subdivided as Symmetric and Asymmetric cryptographic systems, where there is also the classification into stream and block ciphers (the crypted code). Most of the algorithms from this basis of classification are AES, DES, RSA, 3-DES, Blowfish.

II. LITERATURE SURVEY

A secure network must support all security properties. Encrypting of confidential/important documents or any sorts is must as content present in a document if leaked can lead to unwanted results which no one wants to face and to secure files various encryption standards are used. Most of them are of two types: symmetric and asymmetric algorithms, which are still being used. Many algorithms have been developed till now and are still being developed such as DES, Blowfish etc. These two has taken their place as most difficult ones to be decrypted.

A. Data Encryption Standard:

DES is symmetric key block Cipher, which is implementation of Feistel Cipher. Feistel cipher is used to create block cipher which have symmetric structure and DES performs 16-rounds for 64 bits of key length and these rounds are follows the principles of feistel structure in which block size is of 64 bits out of which 8 bits are used as check bits and rest 56 bits are used for encryption as in [13][14].

B. Advanced Encryption Standard (AES):

To overcome the flaws of Data Encryption Standard (DES), Advanced Encryption Standard (AES) was introduced. Similar to DES, AES is also symmetric key cipher and uses variable key lengths (128/192/256 bit). Unlike DES which uses 16 rounds of feistel cipher as in [2], AES has variable count of rounds which are strictly and solely dependent over key kength; for 128 bit key length this algorithm performs 10 rounds. Similar is the case for both 192 bits length key and 256 bits length key where total rounds performed are 12 and 14 rounds respectively.

TABLE I. Basic comparison obtained for AES and DES

Parameters	**DES**	**AES**
Data block division	Divided into two halves	No division (processed as single matrix)
Principle	Feistel Cipher	Substitution and Permutation
Length of plaintext	64 bits	128/192/256 bits
Key length	Smaller than AES	Larger key size than DES
No. of rounds	16 rounds for 64 bits length	10,12 and 14 rounds for128,192,256 bits length respectively.
Speed	Comparatively slow	Faster than DES
Secure	Easy to break (less secure)	Way more secure than DES

C. Rivest-Shamir-Adleman (RSA):

RSA is named after its three founders known by the name Rivest, Shamir & Adleman. It is an asymmetric cryptographic algorithm and is also one of the most popular public key cryptosystems. Its cryptosystem is based upon block cipher system. RSA uses prime numbers (two) to generate public and private key whose length can vary from 1024 bits to 4096 bits, further these keys are used for encryption and decryption. Where sender encrypts the message with the use receiver public key and it can be decrypted with its own private key.

Tables II. Comparison of RSA and DES

Parameters \ Algorithm	**DES**	**RSA**
Memory Used	18.2 KB	31.5
Entropy per byte (encrypt)	2.9477	3.095
Cryptographic algorithm type	Symmetric	Asymmetric
Speed (large data size)	Fast	Too slow
Number of keys used	One	Two
Throughput	Very high	Low
Confidentiality	High	Low
Block Size	64 bits	512 bits (minimum)
Scalability	Yes	No
Power Usage	Low	High
No. of rounds	16	1

D. Triple DES (3-DES):

A symmetric key cryptography technique as in [5], applying three times to each data block. The security is maintained throughout because of increase in key size of DES without designing a new block using bundle of three keys (56 bit each); k1, k2, k3 excluding parity bits and encryption and decryption occurs as:

Ciphertext = EK3(DK2(EK1(plaintext))) and

Plaintext = DK1(EK2(DK3(ciphertext)))

E. BLOWFISH:

Encryption occurs through a 16-round feistel network. BLOWFRISH is a symmetric block cipher of 64-bits. It works by expanding and converting 448 bits of key length (maximum) into key arrays and encrypting through Feistel network of 16 rounds consisting of key dependent permutation and data independent substitution as in [3][6]. It includes key-dependent S-boxes and key structure with high complexity.

F. TWOFISH:

Successor to BLOWFISH [8][9], with 128 bits block size and extending to 256 key size, having Feistel structure like DES as in[3][4], but much secure in comparison to other algorithms with no cryptanalysis yet to be found possible.

TABLE III. Comparison of Triple DES and BLOWFISH

Parameters \ Algorithm	**3DES**	**BLOWFISH**	**TWOFISH**
Key Length	112 and 168 bits (internally)	32 to 448 bits	128 bits 192 bits 256 bits
Block size	64 bits	64 bits	128 bits
Keys	3	Public	Public
Possible keys	2^{112} or 2^{168}	2^{32} or 2^{448}	256
Attacks prone to	Differential , brute force attack	Second order Differential, brute force attack	Highly secure with still no cryptanalysis found

III. IMPLEMENTATION

On the basis of obtained results from different papers, comparison tables have been laid out to obtain the best analysis for the suitability and easiness. Accordingly, we implement these algorithms in JAVA (platform independent language) for its working and obtaining results for encryption and decryption.

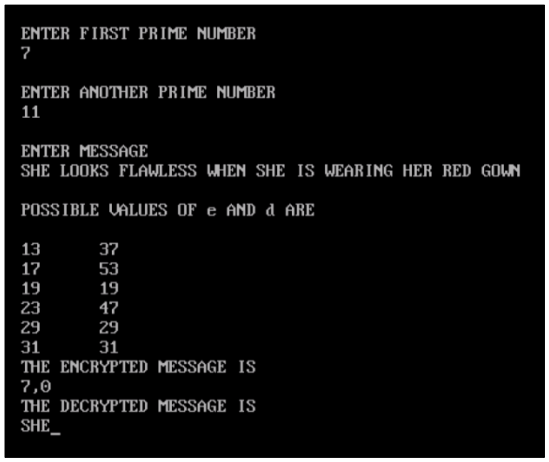

Fig.1. RSA program for a message "She looks flawless when she is wearing her red gown"

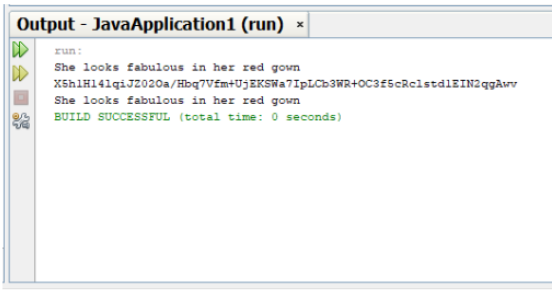

Fig.2. AES program for the same message

Fig.3. Blowfish program for the same message

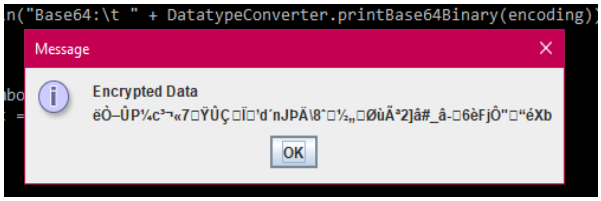

Fig.4. DES program for the same message

The comparison is obtained between basic algorithms AES and DES as in [7][15] then, RSA and DES, after which 3-DES, BLOWFISH s in [10], TWOFISH for obtaining the best security protocol such that DES being popular and highly known has become prone to attacks and being slower, easy to break algorithm is overtaken by RSA (Rivest, shamir and Adelman Algorithm) a well-known cryptographic algorithm obtained to make the decryption as in[11][12] much more difficult by using prime numbers set as the basis with less prone to attacks in comparison where TWOFISH slightly slower than AES when compared in 128 bits but faster for 256 bits,

Table IV. Comparison based on memory, entropy of encryption and optimal encoding through survey and implementation

Algorithm	Memory used (KB)	Entropy/byte of encryption (avg)	Bits /byte for optimal encoding (avg)
DES	18.2	2.9477	27
3DES	20.7	2.9477	40
AES	14.7	3.84024	256
Blowfish	9.38	3.93891	128
RSA	31.5	3.0958	44

Table V. Comparison on the basis of survey and implementation of AES, DES, 3-DES, BBLOWFISH and TWOFISH

Parameters\Algorithm	AES	DES	3DES	BLOWFISH	TWOFISH
Key Length	128,192 or 256 bits	56 bits	112 and 168 bits (internally)	32 to 448 bits	128 bits 192 bits 256 bits
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	128 bits
Block size	128,192 or 256 bits	64 bits	64 bits	64 bits	128 bits
Keys	1	1	3	Public	Public
Possible keys	2^{128},2^{192} or 2^{256}	2^{56}	2^{112} or 2^{168}	2^{32} or 2^{448}	256
Attacks prone to		Differential and linear cryptanalysis	Differential, brute force attack	Differential, brute force attack	Highly secure with still no cryptanalysis found

IV. CONCLUSION

From the literature survey we reviewed and comparisons made with our results it can be said that every encryption has its own strength and weaknesses, almost every encryption is breakable theoretically but we need to find which one is most suited to our need. So, from all information we got it can be said AES and TWOFISH are two best options which can serve the purpose as these two beat rest of encryptions standards in term of speed, entropy, optimal encoding, but

between them AES still has an upper hand due it is efficiency which is more than TWOFISH.

REFERENCES

[1] Shailendra Singh Gaur, Shivani Gautam, Hemanpreet Singh Kalsi "Trusted and secure Wireless Sensor Network using Cryptographic Algorithm and its comparative analysis" published in national conference of computing computation and informatics 2018 (NCCIN2K18 ID-81).

[2] C. Sanchez-Avila, R. Sanchez-Reillol "The Rijndael block cipher (AES proposal): a comparison with DES" Published in**:** Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186)

[3] M. Anand kumar and Dr. S.Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms", I. J. Computer Network and Information Security, 2012, 2, 22-28, Published Online March 2012 in MECS, DOI: 10.5815/ijcnis.2012.02.04, Copyright © 2012 MECS, I.J. Computer Network and Information Security, 2012, 2, 22-28

[4] Bruce Schneier, John Kelsey, Doug Whiting‡ David Wagner, Chris Hall, Niels Ferguson k; "Twofish: A 128-Bit Block Cipher**",** published in Schneier on Security, June 15, 1998.

[5] Hemme L. (2004) A Differential Fault Attack Against Early Rounds of (Triple-)DES. In: Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004. CHES 2004. Lecture Notes in Computer Science, vol 3156. Springer, Berlin, Heidelberg

[5] Simar preet singh, and Raman maini, "Comparison of data encryption algorithms" published in International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[6] Priyadarshini Patil, Prashant Narayankar, Meena S. M. and Narayan D.G. "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish" Published in Elsevier, Procedia Computer Science, Volume 78, 2016, Pages 617-624

[7] Biham, E., Shamir, A: Differential cryptanalysis of DES –like cryptosystems, Journal of Cryptography 4(1), 3-72 (1991)

[8] Shun-Lung Su, Lih-Chyau Wuu, and Jhih-Wei Jhang, "A New 256-bits Block Cipher –Twofish256"

[9] Deepali D. Rane, "Superiority of Twofish over Blowfish", published in International Journal of scientific research and management (IJSRM) ISSN (e): 2321-3418 IJSRM volume 4 issue 11 Nov 2016, Page 4744

[10] Harsh Kumar Verma, Ravindra Kumar Singh, "Blowfish and DES Block Cipher Algorithms Performance Analysis of RC5", published in International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012

[11] Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 513–525. Springer, Heidelberg (1997)

[12] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall, New Jersey, 1999.

[13] H. Feistel, W.A. Notz, and J.L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Communications", Proceedings on the IEEE, v. 63, n. 11, 1975, pp. 1545 -1554.

[14] Shailendra Singh Gaur1, A. K. Mohapatra2 and Sarfaraz Masood3, "Design of an Optimized Novel Cryptographic Algorithm and Comparative Analysis with the Existing Cryptographic Algorithms" I J C T A, 9(34) 2016, pp. 503-514, International Science Press.

[15] Matsui, M.: On Correlation Between the Order of S-boxes and the Strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995)

Shailendra Singh Gaur is currently an Assistant Professor of Information Technology at Bhagwan Parshuram Institute of Technology, GGSIPU in Delhi. Prior to joining as Assistant Professor in BPIT, he has worked as a Lecturer at Ch. Brahm Prakash Govt. Engg. College, GGSIPU and Bhai Parmanand Institute of Business Studies, GGSIPU on Diverted Capacity. He has Industrial experience in Triport Electronic Private Ltd. as Testing Engineer in Noida. His research interest includes Network Security, Computer Network and WSN.

Hemanpreet Singh Kalsi is currently a final year student of Computer Science and Engineering at Bhagwan parshuram Institute of Technology, GGSIPU in Delhi. He is working over cryptography, WSN and network security.

Shivani Gautam is currently a final year student of Information Technology at Bhagwan parshuram Institute of Technology, GGSIPU in Delhi. He is working over cryptography, WSN and network security.